

Bosbach Wolfgang

Von: CSokolowski@dslv.spediteure.de
Gesendet: Dienstag, 3. März 2015 18:03
An: Bosbach Wolfgang
Betreff: Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
Anlagen: DSLV-Stellungnahme IT-Sicherheitsgesetz.pdf

Sehr geehrter Herr Bosbach,

als Spitzenverband repräsentiert der Deutsche Speditions- und Logistikverband (DSLV) über 16 Landesverbände etwa 3.000 Mitgliedsbetriebe mit 520.000 Beschäftigten, mehrheitlich größere mittelständische und inhabergeführte Speditionen sowie global agierende Logistikkonzerne.

Den Ihnen vorliegenden Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) sieht der DSLV kritisch. Er befürchtet, dass die Unternehmen der Speditions- und Logistikbranche durch das Gesetz erheblich belastet werden, obwohl sie nicht zu den Betreibern „Kritischer Infrastrukturen“ zählen. Die Bundesregierung geht zwar branchenübergreifend von „nur“ 2.000 betroffenen Unternehmen aus. Sie räumt aber selbst ein, dass dies nur eine sehr grobe Einschätzung sei, da die Zahl der betroffenen Unternehmen wesentlich von einer noch zu erstellenden Rechtsordnung abhängt.

Dieses Problem hat auch der Bundesrat erkannt, der darum bittet, im weiteren Gesetzgebungsverfahren dafür Sorge zu tragen, dass zur Schaffung von Planungs- und Rechtssicherheit eine weitere Konkretisierung von unbestimmten Rechtsbegriffen erfolgt, und hier vor allem eine Präzisierung des Begriffs „Kritische Infrastrukturen“ anmahnt.

Zu beachten ist auch, dass die Speditions- und Logistikbranche ein polypolistischer Markt ist, der überwiegend von kleinen und mittleren Unternehmen geprägt wird. Die Transportaufkommen in der Bundesrepublik verteilen sich auf eine große Zahl von Dienstleistern. Bei Ausfall eines und auch mehrerer Speditions- und Logistikunternehmen wird es immer alternative Dienstleister geben, die die Speditions- und Logistikdienstleistung übernehmen können, sodass Versorgungsengpässe oder gar Gefährdungen der öffentlichen Sicherheit nicht entstehen.

Wir erlauben uns daher, Ihnen anbei unsere Stellungnahme an das Bundesministerium des Innern vom November 2014 zu übermitteln und hoffen, dass unsere Position bei Ihrer Beratung des Gesetzentwurfs berücksichtigt wird.

Für einen Dialog stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Christoph Sokolowski

DSLV Deutscher Speditions- und Logistikverband e. V.
Referat Politik und Kommunikation
Platz vor dem Neuen Tor 5, 10115 Berlin
Telefon: +49 (0) 30 2787469-0
Telefax: +49 (0) 30 2787469-9
E-Mail: CSokolowski@dslv.spediteure.de
www.dslv.org

Innenausschuss

Eingang mit 1 Anl. am 06.03.15
1. Vors. m.d.B. um (-195-1)
Kenntnisnahme/Rücksprache
2. Mehrfertigungen mit/ohne Anschreiben
an Abg. BE, Obl. Sekr.

an _____

3. Wv _____ A.Drs.
4. z.d.A. (alphab.-Gesetz- BMI)

Key 6/3

Diese E-Mail enthält vertrauliche und rechtlich geschützte Informationen, insbesondere für im DSLV organisierte Betriebe. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten diese E-Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser E-Mail sind nicht gestattet.





DSLVL · Deutscher Speditions- und Logistikverband e. V. · Postfach 1360 · 53003 Bonn

Bundesministerium des Innern
Referat IT II 1
Alt Moabit 101 D
10559 Berlin

Ihr Zeichen ITII1-17002/7#2
Ihre Nachricht vom 4. November 2014
Unser Zeichen LE/MG
Telefon-Durchwahl 0228 91440-28
Telefax-Durchwahl 0228 91440-728
E-Mail LEickmeyer@
dslv.spediteure.de
Datum 12. November 2014

Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Sehr geehrte Damen und Herren,

gerne macht der Deutsche Speditions- und Logistikverband (DSLVL) von der Möglichkeit Gebrauch, zu dem von Ihnen übermittelten Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) Stellung zu nehmen.

Fünf Werkzeuge sind allerdings zur detaillierten Kommentierung eines 62-seitigen Gesetzes eine sehr kurze Zeit. Wir möchten uns daher vorbehalten, gegebenenfalls weitere Kommentare nachzureichen.

Anwendungsbereich / Definition Kritischer Infrastrukturen

Eine Beurteilung des vorliegenden Referentenentwurfs bezogen auf die Speditions- und Logistikbranche hängt maßgeblich vom Adressatenkreis ab. Eine Konkretisierung durch Rechtsverordnung steht jedoch noch aus.

Die Speditions- und Logistikbranche ist ein polypolistischer Markt, der überwiegend von kleinen und mittleren Unternehmen geprägt ist. Entsprechend der aktuellen Studie „TOP 100 der Logistik“ der Fraunhofer Arbeitsgruppe für Supply Chain Services erwirtschaften die umsatzstärksten 100 Logistikdienstleister etwa 27 Prozent des gesamten Branchenumsatzes. Die Transportaufkommen in der Bundesrepublik verteilen sich also auf eine große Zahl von Dienstleistern.

Bei Ausfall eines und auch mehrerer Speditions- und Logistikunternehmen wird es immer alternative Dienstleister geben, welche die Speditions- und Logistikdienstleistung übernehmen können, sodass Versorgungsengpässe oder gar Gefährdungen der öffentlichen Sicherheit nicht entstehen. Beispiele für den ungestörten Ablauf der Versorgung selbst bei weitgehenden Ausfällen eines Verkehrsträgers sind der letzte Streik der Lokomotivführer ab 5. November 2014 und der Ausbruch des Vulkans Eyjafjallajökull im März 2010. Trotz weitgehender Beeinträchtigungen des Güterverkehrs kam es auch bei diesen Ereignissen zu keinen Versorgungsengpässen.

DSLVL · Deutscher Speditions- und Logistikverband e. V. · Weberstraße 77 · 53113 Bonn
Telefon 0228 91440-0 · Telefax 0228 91440-99 · E-Mail info@dslv.spediteure.de · www.dslv.org

sen. Speditions- und Logistikunternehmen zählen daher nach Auffassung des DSLV nicht zu den Betreibern Kritischer Infrastrukturen und sollten damit vollständig vom Wirkungsbereich des Gesetzes ausgenommen werden. Mindestens aber sollten neben den im Gesetzentwurf ausgeklammerten Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 in jedem Fall auch kleine und mittlere Unternehmen ausgenommen werden.

Meldepflichten bei IT-Sicherheitsvorfällen

Die Pflicht zur Meldung von IT-Sicherheitsvorfällen für Betreiber Kritischer Infrastrukturen berührt vor allem den diskreten Umgang mit Daten, der für Unternehmen durchaus wettbewerbsrelevant ist. Nach dem vorliegenden Referentenentwurf bleibt für den Anwender unklar, wie solche IT-Sicherheitsvorfälle zu spezifizieren und die Meldungen überhaupt zu kontrollieren sind. Es ist bisher auch zu wenig konkretisiert, was eine „bedeutende Störung“ im Sinne des Gesetzes ist.

Eine Verpflichtung für Unternehmen, Beeinträchtigungen ihrer IT-Infrastruktur melden zu müssen, kann nur gefordert werden, wenn diese Meldungen auch geeignet sind, einem berechtigten Schutzzweck zu dienen. Ansonsten stellt der administrative Aufwand zur Erfüllung der umfangreichen Meldeverpflichtungen eine ressourcen- und kostenintensive Mehrbelastung für Unternehmen dar, ohne einen Mehrwert für die Sicherheit zu leisten. Unklar ist jedoch, wie diese insofern unspezifizierten Meldungen, ohne dass zuvor die Beeinträchtigung analysiert, Folgen absehbar oder ihr Ursprung ermittelbar wären, zu einem Sicherheitslagebild beitragen können. Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren, Fehlerquellen aufzudecken und Gegenmaßnahmen einzuleiten, bevor sie freiwillig qualitativ aufbereitete Informationen über relevante Beeinträchtigungen mit Marktteilnehmern und Behörden teilen.

Positiv wird vom DSLV die Einräumung einer Möglichkeit zur anonymen Meldung von IT-Sicherheitsvorfällen gesehen. Dennoch bleibt ein erheblicher administrativer Aufwand zu befürchten, der insbesondere für kleine und mittlere Unternehmen zu einer schweren Belastung führen würde. Bei aller Sicherheit ist die Belastbarkeit der Unternehmen stets im Auge zu behalten.

Mindestsicherheitsstandards für informationstechnische Systeme

Als kritisch erachtet der DSLV zudem die vorgeschriebenen Nachweispflichten der Einhaltung von Mindestsicherheitsstandards, da diese einen Eingriff in die unternehmerischen Prozesse und die unternehmerischen Entscheidungsfreiheiten darstellen. Auch wenn die Berücksichtigung branchenspezifischer Sicherheitsstandards begrüßt wird, werden die Anforderungen an den zu erbringenden Nachweis im Gesetz nur unzureichend konkretisiert.

Grundsätzlich befürwortet der DSLV die Einhaltung von Mindestsicherheitsstandards für informationstechnische Systeme auf freiwilliger Basis. Die Anwendung von Informations- und Kommunikationssystemen betrifft den Kern des außerordentlich kommunikationsintensiven Speditions- und Logistikgeschäfts. Angemessene Sicherheitsvorkehrungen für ihre IT-Sicherheit zu treffen, liegt deshalb schon im Geschäftsinteresse von Speditions- und Logistikunternehmen selbst. So treffen selbstverständlich auch heute schon mittelständische Speditionsunternehmen und Speditionskooperationen, in der Regel zusammen mit ihren Softwarelieferanten und Kommunikationsanbietern, Vorkehrungen zur Erhaltung ihrer IT-Sicherheit.

In verschiedenen Bereichen unserer Branche hat sich eine freiwillige Zertifizierung von Managementsystemen, beispielsweise bei speziellen Güter-, Kunden- und Umweltafordernungen, bewährt. Anwendung und Verbreitung der Regelwerke vollziehen sich im Marktwettbewerb. Auch gibt es bereits einzelne Speditionsunternehmen und Speditionskooperationen, die ein zertifiziertes Informationssicherheitsmanagementsystem eingerichtet haben. Solche freiwilligen Lösungen sind in der Wirtschaft unbedingt vorzuziehen.

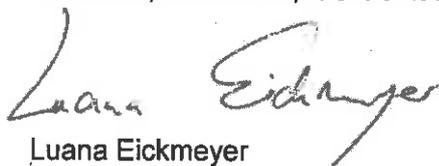
Zusammenfassend begrüßt der DSLV zwar grundsätzlich den von der Bundesregierung angestoßenen Diskussionsprozess zur branchenübergreifenden Verbesserung des IT-Sicherheitsniveaus. Gleichzeitig sind jedoch auch Bedenken an der Schaffung einer nationalen Lösung zu äußern. Globalen Cyberbedrohungen lässt sich effektiv nur mit einem abgestimmten und zumindest europaweit harmonisierten, strategischen Sicherheitskonzept begegnen. Nationalstaatliche Einzelmaßnahmen hingegen bedeuten gerade für weltweit tätige Unternehmen enorme zusätzliche Kosten, ohne dabei einen wirksamen Sicherheitsnutzen zu liefern.

Eine stärkere Zusammenarbeit zwischen Staat, Wissenschaft und Wirtschaft scheint essentiell notwendig, um den wachsenden Bedrohungspotenzialen mit passenden Sicherheitsantworten zu begegnen. Die Speditions- und Logistikbranche ist an verständlich aufbereiteten, aktuellen Informationen zur IT-Sicherheit interessiert. Bezüglich der Meldung von erheblichen IT-Sicherheitsvorfällen weist der DSLV auf die freiwillige Teilnahme von Unternehmen an der „Allianz für Cyber-Sicherheit“ hin, die weiter entwickelt werden sollte. Solch ein Austausch von Informationen fördert die Zusammenarbeit und damit auch das Vertrauen.

Die Sicherheit informationstechnischer Systeme nimmt auch für die Speditions- und Logistikbranche eine zunehmende Bedeutung ein. Ein branchenbezogener Leitfadens könnte für viele, vor allem auch mittelständische Unternehmen, eine Orientierungshilfe bei der Einführung eines Informationssicherheitsmanagementsystems sein. Der DSLV würde es begrüßen, wenn gegebenenfalls auf Unterstützung durch Programme des Bundesministeriums des Innern (BMI) und seiner Ämter, wie beispielsweise dem Bundesamt für Sicherheit in der Informationstechnik (BSI), gerechnet werden könnte. Nach Meinung des DSLV sollten zunächst der Dialog – zwischen BMI, BSI, Branchenverbänden und Unternehmen – wie auch die auf freiwilliger Teilnahme basierenden Maßnahmen zur Verbesserung der IT-Sicherheit vorangebracht werden.

Mit freundlichen Grüßen

DSLVL Deutscher Speditions- und Logistikverband e. V.
Referat Marktbeobachtung und Statistik /
Prozesse, Standards, Elektronischer Geschäftsverkehr


Luana Eickmeyer